DECISION SCIENCES INSTITUTE

Enhancing the Security of Information Systems: A Failure Mode Effects Analysis Approach

Arben Asllani
The University of Tennessee at Chattanooga
Email: beni-asllani@utc.edu

Alireza Lari
Wake Forest University
Email: laria@wfu.edu

Nasim Lari
IBM
Email: nasim.lari@gmail.com

ABSTRACT

This paper views Information Technology (IT) security as a quality matter and its vulnerabilities as potential failure modes. The likelihood that IT vulnerability is exploited and a threat is detected are viewed, respectively, as degree of occurrences and detections. Failure Mode and Effect Analysis (FMEA) identifies risks of failure modes through estimation of severity and occurrence. This paper uses FMEA as a security management tool for IT, discusses several failure modes of IT security, and introduces a step-by-step cyber-FMEA (C-FMEA) methodology. A case study is presented to demonstrate the applicability of the proposed C-FMEA.

KEYWORDS: Information Technology Security, FMEA, Case Study, Airport Security

INTRODUCTION

Considering the importance of secure information systems, the National Institute of Standards and Technology (NIST) has developed security controls (NIST, 2013) for information systems in federal, private and public organizations. NIST has also developed general guidelines (NIST, 2002), for federal government (NIST, 2006), and for non-government organizations (NIST 2011), for managing the risk of information technology systems. Current controls and guidelines mostly assume that the appropriate protection of the information systems security lies in risk management, a process where risk factors are identified and then gradually eliminated. This paper offers a different approach to cyber security. It advocates that security is ultimately a quality matter and requires a quality and reliability engineering approach, such as FMEA to assess, monitor, and mitigate cyber security threats.

This paper is organized as follows. First, there is a brief literature review on the discussion of FMEA and its applications, advantages of using FMEA as an approach to cyber security, and a brief discussion of using FMEA to assess information systems threats, risk, and as a security tool. Then, the section on theoretical foundation and development of the model offers a discussion of information security and how confidentiality, integrity, and availability can be viewed as a quality matter, and the proposed methodology and specific steps to be followed when implementing FMEA for cyber security. A fictional example of an airport is presented next to demonstrate the implementation of FMEA to mitigate the risks of cyber security threats.

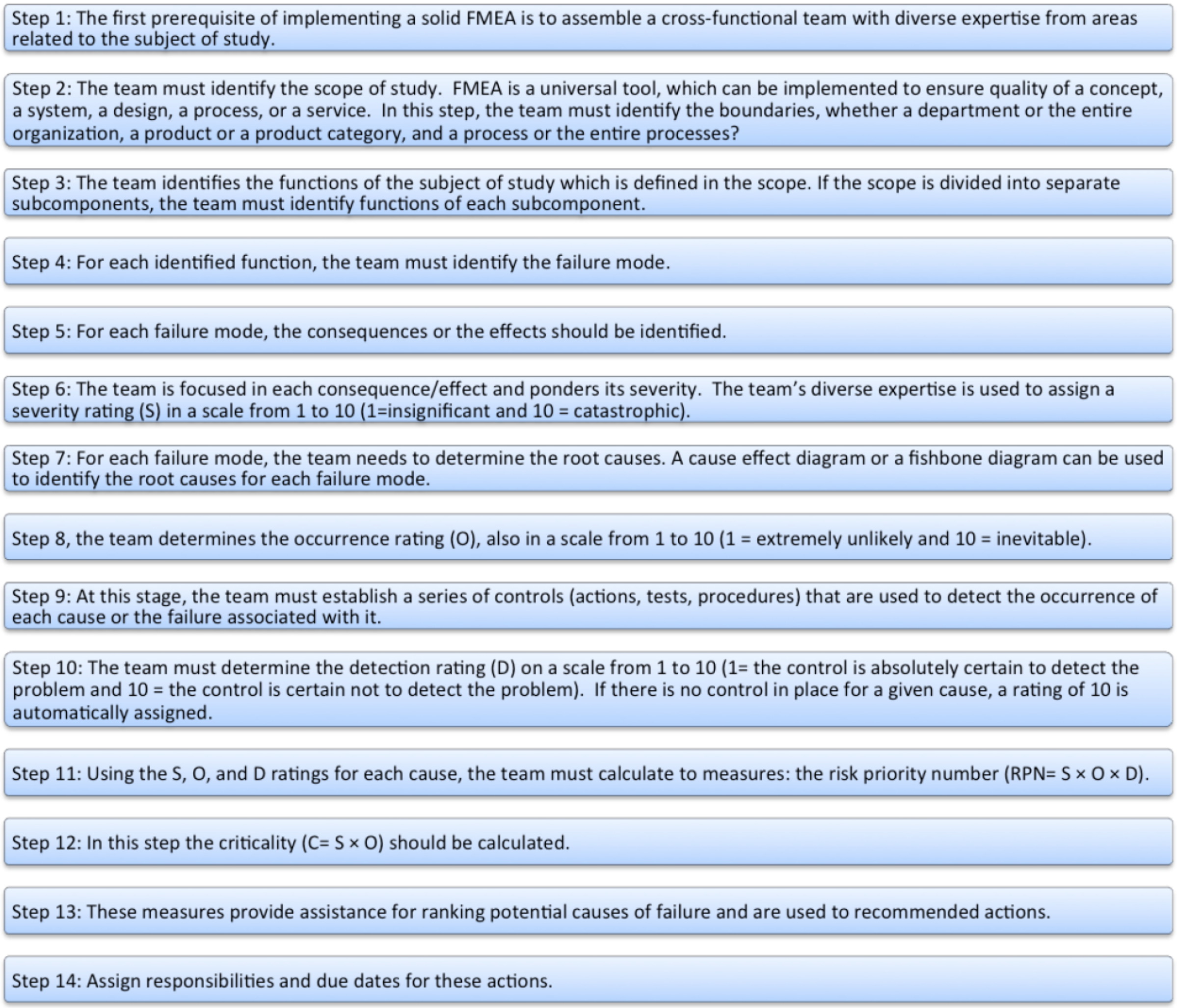
Finally, a section on conclusions offers a roadmap for other organizations that want to implement FMEA to better secure their information systems and related issues.

LITERATURE REVIEW

FMEA and its Applications

FMEA has been used for many applications as a quality management tool. The technique was created by the aerospace industry in the 1960s and is used extensively by Six Sigma practitioners as a tool to quantify and prioritize risk within a process, product, or system and then track actions to mitigate that risk. An early application of FMEA goes back to 1972 when Ford Motor Company used it to analyze engineering design (Foster, 2007). FMEA is a risk management methodology for identifying a system's failure modes, with their effects and causes, and for tracking actions taken. FMEA identifies potential weaknesses in the system. It looks at ways that a system may fail, evaluates the effect of the failure on performance and safety of the system, and rates the seriousness of the failure. As a result of this examination, FMEA creates a higher degree of reliability in the system. Essentially this approach allows companies to correct areas identified through the process before the system fails. Foster (2007) discussed some benefits of FMEA implementation as: improving the safety, reliability and quality of products; recording actions taken to reduce a product risk; and reducing product development cost. Figure 1 shows a summary of a typical FMEA methodology briefly explained below (ASQ, 2016).

Figure 1: FMEA Methodology According to ASQ



Step 1: The first prerequisite of implementing a solid FMEA is to assemble a cross-functional team with diverse expertise from areas related to the subject of study.

Step 2: The team must identify the scope of study. FMEA is a universal tool, which can be implemented to ensure quality of a concept, a system, a design, a process, or a service. In this step, the team must identify the boundaries, whether a department or the entire organization, a product or a product category, and a process or the entire processes?

Step 3: The team identifies the functions of the subject of study which is defined in the scope. If the scope is divided into separate subcomponents, the team must identify functions of each subcomponent.

Step 4: For each identified function, the team must identify the failure mode.

Step 5: For each failure mode, the consequences or the effects should be identified.

Step 6: The team is focused in each consequence/effect and ponders its severity. The team's diverse expertise is used to assign a severity rating (S) in a scale from 1 to 10 (1=insignificant and 10 = catastrophic).

Step 7: For each failure mode, the team needs to determine the root causes. A cause effect diagram or a fishbone diagram can be used to identify the root causes for each failure mode.

Step 8, the team determines the occurrence rating (O), also in a scale from 1 to 10 (1 = extremely unlikely and 10 = inevitable).

Step 9: At this stage, the team must establish a series of controls (actions, tests, procedures) that are used to detect the occurrence of each cause or the failure associated with it.

Step 10: The team must determine the detection rating (D) on a scale from 1 to 10 (1= the control is absolutely certain to detect the problem and 10 = the control is certain not to detect the problem). If there is no control in place for a given cause, a rating of 10 is automatically assigned.

Step 11: Using the S, O, and D ratings for each cause, the team must calculate to measures: the risk priority number (RPN= S × O × D).

Step 12: In this step the criticality (C= S × O) should be calculated.

Step 13: These measures provide assistance for ranking potential causes of failure and are used to recommended actions.

Step 14: Assign responsibilities and due dates for these actions.

Similarly, the proposed C-FMEA methodology intends to offer the same benefits to the security of information systems: improve the reliability of security measures, recommend and record appropriate actions to mitigate the threats, and overall improvement of the efficiency and reducing the cost of cyber security.

In the proposed C-FMEA methodology, we also recommend adding a responsibility matrix, which maps the actions or controls (from step 9) to the assigned people responsible for implementation of such controls. FMEA is an iterative approach and as actions are completed, the team must record the results and modify the values of S, O, and D (calculated in steps 6, 8, and 10) in the next iteration.

Using FMEA for Risk Assessment and Cyber Security

Since 1980, military standards (MIL-STD-1629A) have considered information security as a quality issue and have recommended using FMEA to monitor threats and other failure causes (US Department of Defense, 1980). Shirouyehzad, Dabestani, and Badakhshian (2011) suggest use of FMEA to identify critical failure factor to improve reliability of the "big ticket" information system, the enterprise resource planning system (ERP). They find that FMEA provides a higher degree of reliability in the system and can reduce the need for modifications to the design, provide product improvement on a continual basis and reduce manufacturing costs. Most recently, Muckin & Fitch (2014) of Lockheed Martin Corporation offer a “threat-driven” approach to cyber security and recommend using FMEA to monitor the security of an information system. Also, Silva, Gusmão, Poleto, Silva , & Costa (2014) use FMEA to analyze the security threats. This approach analyses five dimensions of information security: access to information and systems, communication security, infrastructure, security management and secure information systems development. In other applications, Mandal & Maiti (2014) use FMEA for risk analysis and Patel, Grahamb, & Patricia (2008), offer a method to quantify risk in terms of a numeric value or degree of cyber security.

Zafar, Mehboob, Naveed, & Malik (2015), consider security as a matter of quality and propose a quality model to enhance software security. They use a quality framework, which was originally proposed by Dromey (1995), to identify known security defects, their fixes, and the underlying low-level software components along with the properties that positively influence the overall security of the product.

THEORETICAL DEVELOPMENT/MODEL

CIA Triad and Failure Modes

From a security perspective, a high quality information system ensures information confidentiality, integrity, and availability, also known as the CIA triad (Perrin, 2008, and Gibson, 2011). In the following section, these factors are briefly explained with their potential failures, the information system components where these failures might occur, and the triggering actions that can help to avoid such failures.

Confidentiality

The quality standard of confidentiality and privacy aims to protect data from being viewed or disclosed to unauthorized parties. One of the confidentiality principles is to provide access to data and information only to the authorized people with a defined and specific need to see or use that information. Some of the possible failure modes regarding confidentiality include: disclosing data to unauthorized parties, collecting unauthorized information about customers, anonymizing or masking sensitive data, illegal intrusion to data and information, not locking files properly, not removing identifiers from questionnaires or electronic data files, or not encrypting files containing identifiers (National Research Council, 2005). Each of these confidentiality failure modes can be avoided by proper defensive actions. For example, cryptography and encryption methods are to ensure the confidential transmission of data from one computer or system to another. Cryptography hides or codes the information as it is being transmitted on a network and encryption ensures that unauthorized users do not read data since only those who hold the encryption key can decrypt the information.

Integrity

The quality standard of integrity of IT systems aims to guarantee that the information: is modified and destroyed only by authorized parties; is modified and destroyed only in authorized ways; is assumed to be authentic, i.e. authorized parties can be verified; and any change of information cannot be repudiated, i.e. cannot be denied by the authorized changing party.

There exist several measures to provide end-to-end data integrity. These measures include installation of antivirus programs, establishing authenticity and non-repudiation protocols, applying “check-sum” procedures, installation of system and data recovery utility software programs. Malware is a common root cause of data corruption and it can cause intentional or unintentional loss of data integrity. A virus also alters files and renders an information system unusable. A “check-sum” procedure can be used to detect and correct possible data corruption. Other programs can repair the corrupted file automatically, depending on the level of corruption. In more extreme cases, when data seems to be uncorrectable, one can apply automatic restoration from backups.

Availability

The quality standard of availability aims to make data and information available to the authorized users when it is needed. Very often, data is time-sensitive and the value may diminish if delayed. A typical failure mode for availability of a system occurs when access to the information is delayed or denied due to denial of services attacks, power outages, floods, fires, or other environmental or man-made disasters. The best corrective actions to ensure data availability are regular data backups, off-site data storage, redundant parallel systems, and physical protection of information systems. The discussion is summarized in Table 1.

Proposed C-FMEA Approach

In this section, the FMEA approach is intuitively attuned to mitigate the cyber security threats. The Cyber RPN (CRPN), in such a case, is a product of the cyber threat impact (in a scale from 1 to 10), the chance that the cyber threat will happen (in a scale of 1 to 10), and the chance that the cyber threat can be detected (also in a scale of 1 to 10). The CRPN can be used to generate corrective actions, and also to set cyber threat goals and assure that these goals are achieved with appropriate cyber defensive strategies.

We use FMEA to incorporate security issues into the design of an IT system. In order to achieve the above objectives, the steps are suggested in Figure 2. The proposed steps will be explained in more details with the case presented in the next section.

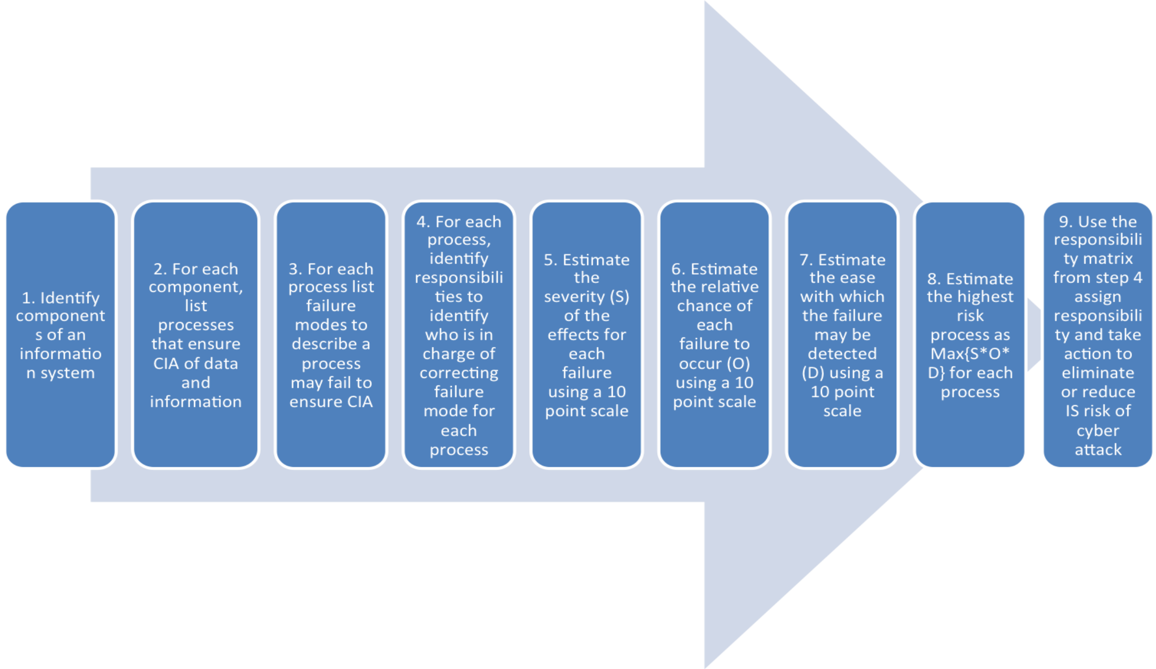
Table 1: Security as a Quality Attribute

Security Dimension	**Failure Modes**	**Corrective Actions**
Confidentiality	• Unauthorized user has access to data and information	• Physical protection of computer systems and its components • Security training of end-user
	• Unauthorized information is stored and transmitted	• Data encryption • Security training of end-user
	• Sensitive data is not encrypted or coded	• Data encryption • Implementation of security protocols, such as SSL/TLS
	• Data is illegally intruded • Files are not locked properly	• Application of "need-to-know" or "least privilege" guidelines • Security training of end-user
	• Identifiers are not removed from data records as those records are analyzed and processed into reports	• Security training of end-user • Application of "need-to-know" or "least privilege" guidelines
Integrity	• Lack of data authenticity and repudiation	• Implement a “check-sum” procedure
	• Data corruption when writing, reading, storing, or transmitting	• Timely update operating system and software programs • Apply automatic restoration from backups
	• Presence of malware or virus in the system	• Install antivirus software and periodically scan the system
Availability	• Access to information is delayed	• Regular data backups • Off-site data storage • Redundant parallel systems • Physical security of information systems
	• Access to information is denied due to denial of services attacks	• Implementation of security protocols, such as SSL/TLS
	• Hacking attacks	• Physical protection of computer systems and its components • Security training of end-user
	• Power outages, floods, fires, man-made disasters	• Regular data backups • Off-site data storage • Redundant parallel systems • Physical security of information systems

IMPLEMENTATION OF C-FMEA IN A REGIONAL AIRPORT

Information systems have become the driving force of the airport infrastructure. Such heavy dependency of airport operations on hardware, software, data, and networks has a dual and opposing impact on airport security: while the technology has become beneficial to enhance the security of airport operations, at the same time it poses vulnerabilities to potential cyber-attacks (Asllani & Ali, 2011). For example, the common use of terminal equipment (CUTE) is an IT driven-system that allows several airlines to share gates and check-in counters. However, sharing CUTE among several airlines, while increases efficiency and lowers the cost, causes security concerns when airlines share data, protocols, procedures, and information. These concerns are related to firewalls, passwords, intrusion protection, and operational security (Feldman, 2003). C-FMEA methodology presented in Figure 2, demonstrates the ability to address these concerns and enhance the security of information systems. The detailed implementation of the C-FMEA steps for a regional airport is presented below.

Figure 2: Proposed C-FMEA Steps


1. Identify components of an information system
2. For each component, list processes that ensure CIA of data and information
3. For each process list failure modes to describe a process may fail to ensure CIA
4. For each process, identify responsibilities to identify who is in charge of correcting failure mode for each process
5. Estimate the severity (S) of the effects for each failure using a 10 point scale
6. Estimate the relative chance of each failure to occur (O) using a 10 point scale
7. Estimate the ease with which the failure may be detected (D) using a 10 point scale
8. Estimate the highest risk process as Max{S*O*D} for each process
9. Use the responsibility matrix from step 4 assign responsibility and take action to eliminate or reduce IS risk of cyber attack

Creating a team of experts to implement C-FMEA is the prerequisite for a successful implementation. The system administrator or other information technology personnel are responsible for implementing security measures and, as such, they must initiate, lead the C-FMEA project. However, it is suggested that end-users of the information systems should participate in the systems security projects.

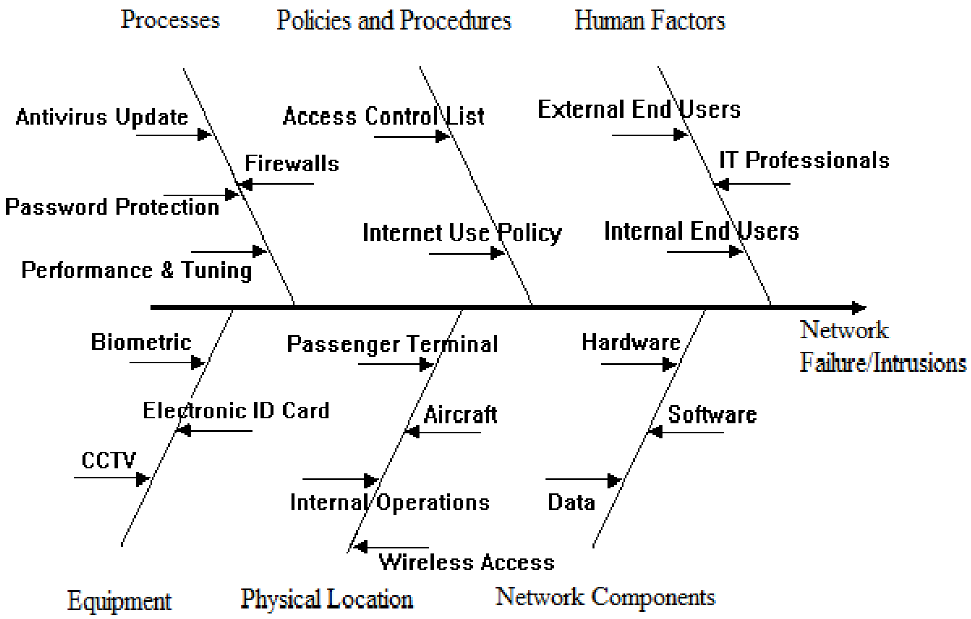
1. Identify components of an information system

Identifying the components of the information systems at the airport helps to decide which aspects of the airport security are most vulnerable to physical break-ins or unauthorized use. Typical components of an airport network as related to security are: security processes, policies and procedures, people, digital devices connected to the network, network components, and physical locations that the components are located.

2. *For each component, list processes and procedures that are necessary to ensure confidentiality, integrity, and availability of data and information*.

Figure 3 illustrates an airport network security problem. Each of the processes listed in Figure 3, when fail to be implemented properly, is a potential source for network vulnerability. In the *process* category, there are four causes of security threats: antivirus software is not updated, passwords are not changed periodically, fireworks are misplacement, and the security administrator has not completed performance testing and tuning periodically. The security *policies and procedures* must also be followed to avoid possible network failures, unwanted intrusions, and threat of CIA. There are three categories of people in the *human factor* component involved in the airport network security. The first category is passengers, which are considered external end-users and operate in the check-in and boarding areas. The second category is the airport security personnel and airline employees, also known as internal end users. The third category is IT personnel. C-FMEA approach considers any member of these groups as a potential cause that can jeopardize the security of the network, either unintentionally or intentionally.

Figure 3: List of Processes and Procedures to Ensure CIA



The *equipment* component lists several network devices that are used to physically secure the airport operations. Examples of these devices include electronic ID cards, closed circle TVs, or biometric measurement devices. When used improperly, the network security devices can jeopardize the security of the airport network. Figure 3 also identifies major causes of network security breach related to *physical locations.* These areas include the area around the gates and aircraft, the terminal, the internal operation zone, and the back office. Finally, each *network component* is a potential cause for security intrusion or failure.

3. *For each process, list potential failure modes as they relate to CIA triad*

Table 2 indicates potential failure modes for each network security process at the airport as relate to the three components of security. For this exercise, we have indicated one or more failures based on the general understanding of airport security matters. Each airport network has its own specifics and the team created for each C-FMEA project identifies the failure modes.

4. *For each process, identify the responsibilities of person (s) in charge of correcting failure mode for each process*

These responsibilities are summarized in Table 3. Antivirus updates must be performed by everyone in the organization, and firewall protection must be established by the airport IT professionals and network administrators. Internal users must always change their passwords and network administrator must set password requirements and enforce them continuously. IT professionals, database administrators and network administrators must ensure that the IT network performs at its full capacity and is always up-to-date with the latest software releases. Database and network administrators review the access control list (ACL) and formulate and enforce end-user and Internet access policies while internal users are responsible for implementing such policy.

Table 2: Failure Modes as Related to the CIA Triad

Security Processes	**Failure Modes**		
	Confidentiality	**Availability**	**Integrity**
Antivirus Update			x
Firewall		x	
Password Protection	x		
Performance and Tuning			x
Access Control List	x	x	
Internet Use Policy	x		x
External Users	x		x
Internal Users	x		x
IT Professionals			x
CCTV	x		
Biometric	x		
Electronic ID Cards	x		
Terminal		x	
Aircraft			x
Wireless Access		x	x
Internal Operations			x
Hardware	x	x	x
Software	x	x	x
Data	x	x	x

IT professionals, database and network administrators, and airport security personnel must enforce security practices and monitor the compliance with such practices of external and internal users, as well as IT professionals at the airport. Secure performance of CCTV, biometric devices, and electronic ID cards are the responsibility of network administrator and the airport security. Airport security and airline employees must enforce proper access to terminal and aircraft. Network administrator must allow a secure access to the wireless network while the security of IT enhanced internal operations is the responsibility of internal users, IT professionals, database and network administrators, and airport security personnel. The network security administrator and other IT personnel must address the potential attacks on hardware and software. Finally, unauthorized access to databases is the responsibility of the database administrator.

5. Estimate the severity (S) of the effects for each failure using a 10-point scale

In a typical risk analysis, the ranking of severity is based on the estimated cost to address or repair a security failure. However, in practice it is difficult to estimate such losses especially when there is no data from previous security breaches. The C-FMEA approach recommends a more practical approach: using the team of experts to estimate a severity score in a scale from 1 to 10. An old but relevant structured communication technique known as the Delphi method (Dalkey & Helmer, 1963) can be successfully used by the C-FMEA team to estimate the values of S for each failure mode. Severity values for each security process are shown in the second column (S) of Table 4.

Table 3: Mapping Security Processes with Security Personnel

Security Processes	Internal Users	IT Professionals	Database Administrator	Network Administrator	Airport Security
Antivirus Update	x	x	x	x	x
Firewall		x		x	
Password Protection	x			x	
Performance and Tuning		x	x	x	
Access Control List			x	x	
Internet Use Policy	x	x		x	
External Users		x	x	x	x
Internal Users		x	x	x	x
IT Professionals		x	x	x	
CCTV				x	x
Biometric				x	x
Electronic ID Cards				x	x
Terminal	x				x
Aircraft	x				x
Wireless Access				x	
Internal Operations	x	x		x	x
Hardware		x		x	
Software		x		x	
Data			x	x	

6. Estimate the relative chance of each failure to occur (O) using a 10-point scale

Security experts and the C-FMEA team can also estimate the likelihood that a failure will occur. For lack of prior experience, we also recommend the use of Delhi method. The chance of occurrence for each failure can also be revised in lieu any news or intelligence reports on potential security threats. The estimated values of the chance of occurrence are shown in the third column (O) of Table 4.

7. Estimate the ease with which the failure may be detected (D) using a 10-point scale

A similar approach as in steps 5 and 6 (Delphi method, team's expertise, cyber intelligence reports) can be used to estimate the degree of detecting a cyber-security attack. These values are shown in the fourth column (D) of Table 4.

Table 4: Calculating CRPN for Each Security Failure at the Network

Failure Causes	**S**	**O**	**D**	**CRPN**
Antivirus Update	3	5	6	90
Firewall	7	3	4	84
Performance and Tuning	2	7	5	70
Password Protection	4	7	3	84
Access Control List	5	2	8	80
Internet Use Policy	6	2	7	84
Internal Users	3	6	4	72
IT Professionals	2	4	5	40
CCTV	3	2	6	36
Biometric	3	4	8	96
Electronic ID Cards	2	3	4	24
Terminal	3	3	1	9
Aircraft	3	3	1	9
Internal Operations	3	7	4	84
Wireless Access	4	8	3	96
Hardware	2	4	4	32
Software	2	2	3	12
Data	3	4	6	72

*8. Estimate the highest risk process as the maximum of {S*O*D} for each process*

The cyber risk priority number (CRPN) is calculated by multiplying the severity (S), occurrence (O), and detection (D) and the results are shown in the fifth column of Table 4.

9. Use the responsibility matrix from step 4 to assign responsibility and take actions

Ghosh (2010) recommends that corrective actions be taken for any process or component with CRPN value exceeding 80. The corrective action ideally leads to a lower CRPN number. Once the priorities are calculated, a detailed plan of action can be generated. The information systems components and each potential failure mode are listed with its CRPN number in Table 5. For example, firewall updates, password protection measures, the Internet use policy enforcements, internal operations security reviews, antivirus updates, biometric devices security, and wireless security are considered significant threats (CRPN >80) and as such priority dates are assigned to deal with these threats. For each action, details about start date, completion date, and person responsible are provided.

At this stage of the C-FMEA project, the responsible party implements specific security measures to address the causes of failure. Such actions include random security controls, or updating the digital devices such as scanners, metal detectors, and backscatter x-rays (Holbrook, 2010).

As the operational plan is executed, the new set of values for S, O, and D are calculated and a new list of recommendations for future actions is prepared. Implementation of the C-FMEA project provides insights and lessons for the airport security administrators. For example, the network administrator can generate guidelines about training procedures, improve Internet use policy, and revise security measures to physically protect network facilities.

RECOMMENDATIONS AND CONCLUSIONS

This paper offers a unique approach to managing the security of the information systems. The proposed C-FMEA methodology has several advantages compared to traditional risk management approaches. The main thrust of the paper is the consideration that security is a quality matter, i.e., a high-quality information system is the one that processes, communicates, and produces data with a high level of confidentiality, integrity, and availability. The proposed methodology incorporates these three dimensions of IT security into the traditional FMEA approach already used in other manufacturing or service systems. The process of protecting the organizational networks and their information systems is a continuous process. As such, we propose that C-FMEA must be treated as a continuous project. System administrators and consultants can use the approach to analyze any vulnerability in an existing information system and to offer proactive recommendations to protect the system against potential threats.

The proposed C-FMEA is a qualitative and systematic tool, usually created within a spreadsheet, to help practitioners anticipate what might go wrong with an information system in general or its components. In addition to determining how an information system might fail, C-FMEA also helps find the possible causes of failures and the likelihood of failures being detected before their occurrence. The ability to anticipate security issues early allows cyber security administrators to prevent potential failures or vulnerabilities. The proposed methodology is demonstrated using a fictional airport. This was a learning exercise and we intend to implement the methodology in a real case environment.

Table 5: Action Plan Recommended by C-FMEA Project

IS Component	Failure Causes	CRPN	Person Responsible
Processes	Antivirus Update	90	Internal Users IT Professionals Network Administrators
	Firewall	84	IT Professionals Network Administrators
	Performance and Tuning	70	IT Professionals Database Administrators Network Administrators
	Password Protection	84	Internal Users Network Administrators
Policies and Procedures	Access Control List	80	Database Administrators Network Administrators
	Internet Use Policy	84	Internal Users IT Professionals Network Administrators
Human Factors	Internal Users	72	IT Professionals Database Administrators Network Administrators Airport Security
	IT Professionals	40	IT Professionals Database Administrators Network Administrators
Equipment	CCTV	36	Network Administrators Airport Security
	Biometric	96	Network Administrators Airport Security
	Electronic ID Cards	24	Network Administrators Airport Security
Physical Location	Terminal	9	IT Professionals Airport Security
	Aircraft	9	IT Professionals Airport Security
	Internal Operations	84	Internal Users IT Professionals Network Administrators Airport Security
Network Component	Wireless Access	96	Network Administrator
	Hardware	32	IT Professionals Network Administrators
	Software	12	IT Professionals Network Administrators
	Data	72	Database Administrators Network Administrators

**Note:* Expected Start and Completion dates are not shown here.*

REFERENCES

Asllani, A., & Ali, A. (2011). Securing information systems in airports: A practical approach. 6th International Conference for Internet Technology and Secured Transactions (pp. 314-318).

ASQ. (2016, November 22). Failure mode effects analysis (FMEA). Retrieved January 14, 2017, from ASQ Web site: http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html

Dalkey, N., & Helmer, O. (1963). An Experimental Application of the DELPHI Method to the Use of Experts. Management Science, 458 - 467.

Dromey, R. G. (1995). A model for software product quality. IEEE Transactions on Software Engineering, 21 (2), 146 - 162.

Feldman, J. (2003). First-class IT service. Network Computing, 14 (7), 44-49.

Foster, T. S. (2007). Managing Quality: Integrating the Supply Chain (5th Edition). New Jersey, NJ: Prentice Hall.

Ghosh, M. (2010, September 26). Process Failure Mode Effects Analysis (PFMEA). Retrieved January 5, 2017, from Process Excellence Network: http://www.processexcellencenetwork.com/business-process-management-bpm/articles/process-failure-mode-effects-analysis-pfmea

Gibson, D. (2011, May 27). Understanding the Security Triad (Confidentiality, Integrity, and Availability). Retrieved January 6, 2017, from Pearson IT Certification: http://www.pearsonitcertification.com/articles/article.aspx?p=1708668

Holbrook, E. (2010). Airport Security: Privacy vs. Safety. Risk Management, 57 (2), 12-14.

Mandal, S., & Maiti, J. (2014). Risk analysis using FMEA: Fuzzy similarity value and possibility theory based approach. Expert Systems with Applications, 41, 3527–3537.

Muckin, M., & Fitch, S. C. (2014). A Threat-Driven Approach to Cyber Security. Retrieved January 5, 2017, from Lockheed Martin Corporation: http://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/Threat-Driven%20Approach%20whitepaper.pdf

National Research Council. (2005). Risks of Access: Potential Confidentiality Breaches and Their Consequences. In C. o. Panel on Data Access for Research Purposes, Expanding Access to Research Data: Reconciling Risks and Opportunities (pp. 50-62). Washington, D. C.: The National Academies Press.

NIST. (2006). Guide for Developing Security Plans for Federal Information Systems. (Special Publication 800-18). Retrieved December 21, 2016, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

NIST. (2011). Managing Information Security risk. (Special Publication 800-39). Retrieved January 3, 2017, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

NIST. (2013). Recommended Security Controls for Federal Information Systems and Organizations. (Special Publication 800-53, Revision 4). Retrieved December 29, 2016, from National Institute of Standards and Technology: http://disa.mil/services/dod-cloud-broker/~/media/files/disa/services/cloud-broker/nist-sp80053-securityandprivacycontrols.pdf

NIST. (2002). Risk Management Guide for Information Technology Systems (Special Publication 800-30). Retrieved December 29, 2016, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Patel, S. C., Grahamb, J. H., & Patricia, A. (2008). Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. International Journal of Information Management, 28, 483–491.

Perrin, C. (2008, June 30). The CIA Triad. Retrieved January 6, 2017, from IT Security: http://www.techrepublic.com/blog/it-security/the-cia-triad/

Shirouyehzad, H., Dabestani, R., & Badakhshian, M. (2011). The FMEA Approach to Identification of Critical Failure Factors in ERP Implementation. International Business Research, 4 (3), 254-263.

Silva, M. M., Gusmão, A. P., Poleto, T., Silva, L. C., & Costa, A. P. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. International Journal of Information Management, 34, 733-740.

US Department of Defense. (1980, November 24). Military Standard 1629A. Retrieved January 5, 2017, from US Department of Defense: http://www.fmea-fmeca.com/milstd1629.pdf.

Zafar, S., Mehboob, M., Naveed, A., & Malik, B. (2015). Security quality model: an extension of Dromey’s model. Software Quality Journal, 23, 29-54.